(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
8 April 2004 (08.04.2004)

PCT

(10) International Publication Number
WO 2004/030311 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/IB2003/004110

(22) International Filing Date: 22 September 2003 (22.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/414,942	30 September 2002 (30.09.2002)	US
60/445,265	5 February 2003 (05.02.2003)	US

(71) Applicant *(for all designated States except US)*: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: ROSNER, Martin [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US). KRASINSKI, Raymond [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US). EPSTEIN, Michael, A. [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

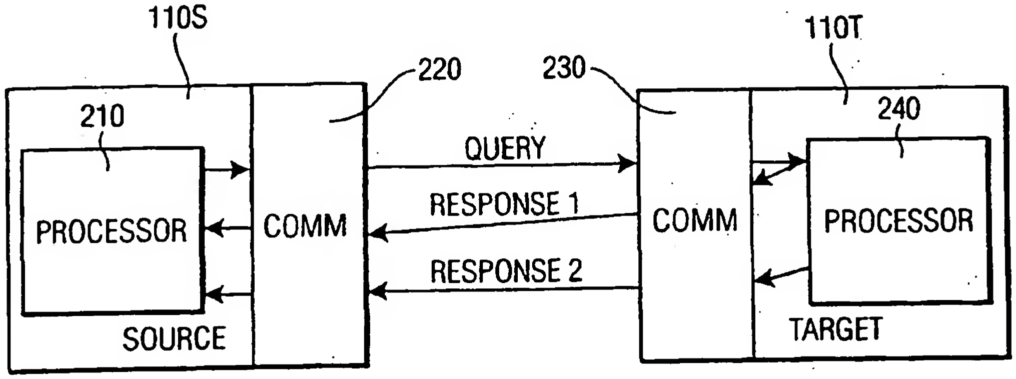
(74) Common Representative: KONINKLIJKE PHILIPS ELECTRONICS N.V.; Intellectual Property & Standards, c/o THORNE, Gregory, L., P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,

[Continued on next page]

(54) Title: SECURE PROXIMITY VERIFICATION OF A NODE ON A NETWORK



(57) Abstract: A system and method determines the proximity of the target node to the source node from the time required to communicate messages within the node-verification protocol. The node-verification protocol includes a query-response sequence, wherein the source node communicates a query to the target node, and the target node communicates a corresponding response to the source node. The target node is configured to communicate two responses to the query: a first response that is transmitted immediately upon receipt of the query, and a second response based on the contents of the query. The communication time is determined based on the time duration between the transmission of the query and receipt of the first response at the source node and the second response is compared for correspondence to the query, to verify the authenticity of the target node.

WO 2004/030311 A1

In accordance with this invention, the target node 110T is configured to provide two responses to the query. The target node 110T provides an immediate response upon receipt of the query, and then a subsequent response after processing the query. The source node 110S is configured to measure the time duration between the transmission of the query and the receipt of the first response from the target node 110T to determine the relative proximity of the target node 110T to the source node 110S. The source node is also configured to verify the authenticity of the target node 110T based on the second response from the target node 110T. In a preferred embodiment, the authenticity of the first response is also verifiable as originating from the target node 110T, either via the contents of the first response or the second response.

Using known techniques, the distance between the source 110S and target 110T can be calculated using the determined communication time between the transmission of the query from the source 110S and the receipt of the first response from the target 110T. As noted above, in a typical embodiment, the communication time is used to determine whether the target 110T is local or remote from the source 110S. This determination is made in a preferred embodiment of this invention by comparing the communication time to a nominal threshold value, typically not more than a few milliseconds. If the communication time is below the threshold, the target 110T is determined to be local; otherwise, it is determined to be remote. Multiple thresholds may also be applied, to provide for a relative measure of the degree of remoteness of the target 110T from the source 110S.

In a typical embodiment, the source 110S uses the remote/local proximity determination to control subsequent communications with the target 110T, and/or to control access of the target node to system resources, such as data and processes, based on the proximity. For example, some files may be permitted to be transferred only to local nodes, all communications with a remote node may be required to be encrypted, some files may be prohibited from inter-continental transmissions, and so on.

In a preferred embodiment of this invention, the above query-response process is integrated within a node-authentication process, such as a key-exchange process, which typically includes one or more query-response sequences.

The OCPS protocol, for example, includes an authentication stage, a key exchange stage, a key generation phase, and subsequent data transmission phases. The key exchange receipt of the query from the source 110S. After sending the first response, the target 110T decrypts the query from the source 110S, using the private key of the target 110T, and generates a new message composed of a new random key and the decrypted random key. The target then encrypts the new message using the public key of the source 110S, signs the message using its private key, and transmits the enrypted and signed response contained in the query back to the source 110S, thereby verifying the identity of the target 110T to the source 110S.

When the source node 110S receives the first response, it terminates the aforementioned timer, thereby establishing a measure of the round-trip communication time between source 110S and target 110T. Upon receipt of the second response, the source node 110S verifies the signed message, using the public key of the target 110T, and decrypts the random numbers and random key from the response, using the private key of the source 110S.

To confirm the key exchange, the source 110S transmits the decrypted new random number back to the target 110T. Both the source 110S and target 110T control subsequent communications based upon receipt of the proper decrypted random numbers. In accordance with this invention, the source 110S also controls subsequent communications based upon the determined communication time.

If both nodes are verified, subsequent communications between the source 110S and target 110T encrypt the communications using a session key that is a combination of the random keys, the public keys, and a session index.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention and are thus within the spirit and scope of the following claims.

6. The method of claim 5, wherein

the first response includes a random number, and

the processing of the query further includes encrypting the item and the random number using a public key of the source node to form at least a portion of the second response.

7. The method of claim 5, wherein

the first response includes an encryption of a random number based on a public key of the source node.

8. The method of claim 1, wherein

determining the proximity includes comparing the communication time to a threshold value that distinguishes between local and remote nodes.

9. The method of claim 1, further including

restricting communications with the target node based on the proximity.

10. The method of claim 1, further including

restricting access of the target node to system resources based on the proximity.

11. A node on a network including:

a communication device that is configured to receive a query from a source node and to transmit a first response that facilitates proximity verification of the node, to the source node upon receipt of the query, and a second response that facilitates a verification of the node to the source node, and

a processor that is configured to process the query and produce therefrom the second response.

12. The node of claim 11, wherein

the processor is configured to process the query and produce the response as part of a cryptographic key-exchange protocol.

19. The node of claim 18, wherein

the processor is configured to generate the query and process at least one of the first and second responses as part of a cryptographic key-exchange protocol.

20. The node of claim 19, wherein

the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol.

21. The node of claim 18, wherein

the query and at least one of the first and second responses correspond to at least a portion of an OCPS protocol initiated by the node.

22. The node of claim 18, wherein

the query includes an encryption of an item based on a public key of the target node, and

the second response includes a decryption of the item based on a private key of the target node.

23. The node of claim 22, wherein

the first response includes a random number, and

the second response includes an encryption of the decryption of the item and the random number, using a public key of the node.

24. The node of claim 23, wherein

the second response further includes a signature of the decryption of the item and the random number, using a private key of the target node.

25. The node of claim 22, wherein

the first response includes an encryption of a random number based on a public key of the node.

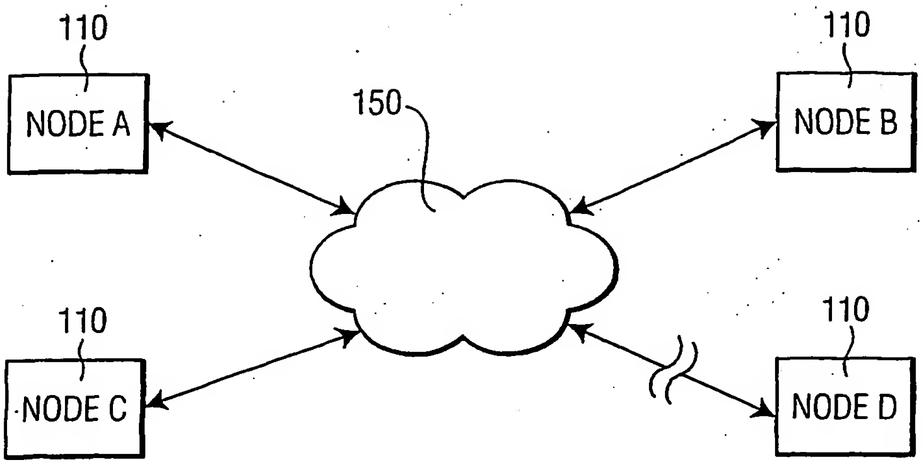

110
NODE A
110
NODE B
150
110
NODE C
110
NODE D

FIG. 1

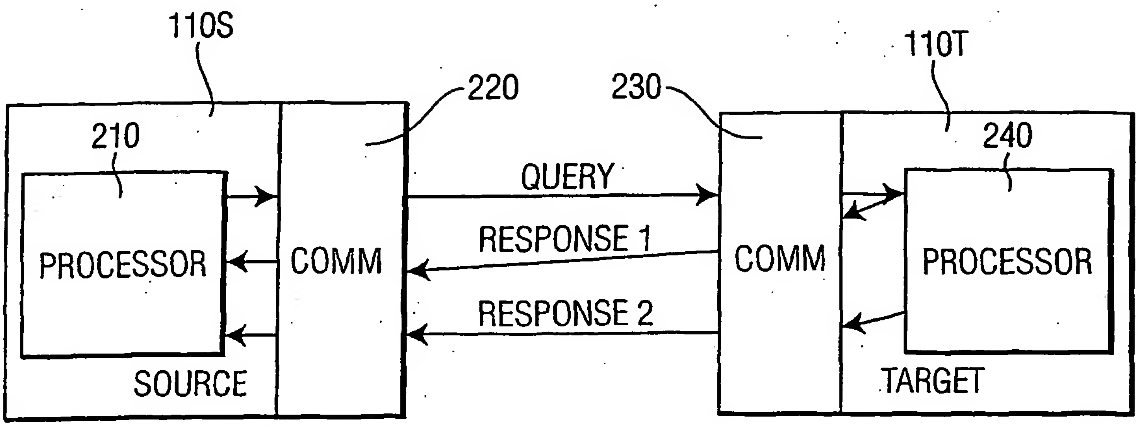

110S
210
PROCESSOR
SOURCE
COMM
220
230
QUERY
RESPONSE 1
RESPONSE 2
COMM
110T
240
PROCESSOR
TARGET

FIG. 2

INTERNATIONAL SEARCH REPORT

rmation on patent family members

Inte al Application No
PCT/IB 03/04110

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
WO 0235036	A	02-05-2002	SE	519748	C2	08-04-2003
			AU	1114102	A	06-05-2002
			EP	1330583	A1	30-07-2003
			SE	0003833	A	24-04-2002
			WO	0235036	A1	02-05-2002
			US	2003184431	A1	02-10-2003
WO 0193434	A	06-12-2001	AU	5882200	A	11-12-2001
			AU	6127701	A	11-12-2001
			AU	6127801	A	11-12-2001
			AU	6300701	A	11-12-2001
			AU	6300801	A	11-12-2001
			AU	6457301	A	11-12-2001
			AU	6457401	A	11-12-2001
			AU	6457501	A	11-12-2001
			AU	7481901	A	11-12-2001
			AU	7482001	A	11-12-2001
			EP	1295405	A1	26-03-2003
			EP	1302001	A2	16-04-2003
			EP	1284049	A1	19-02-2003
			JP	2003535552	T	25-11-2003
			JP	2003535557	T	25-11-2003
			WO	0193441	A1	06-12-2001
			WO	0193442	A1	06-12-2001
			WO	0193434	A2	06-12-2001
			WO	0193519	A1	06-12-2001
			WO	0193482	A2	06-12-2001
			WO	0193443	A2	06-12-2001
			WO	0193444	A1	06-12-2001
			WO	0193445	A2	06-12-2001
			WO	0193520	A2	06-12-2001
			WO	0193446	A2	06-12-2001
			US	2003096578	A1	22-05-2003
			US	2003161411	A1	28-08-2003
			US	6505032	B1	07-01-2003
			US	2003174048	A1	18-09-2003